REMARKS/ARGUMENTS

This supplemental amendment is submitted in response to the Office Action mailed August 24, 2007 for making additional clarifying amendments to the claims and for setting forth additional reasons as to why Applicants rejected claims should be deemed patentable over the cited references. Further, the amendment should place the application in condition for reconsideration and allowance. Claims 15-18 and 20-34 are active in the application

By this amendment, claim 15 has been amended for the purpose of pointing out with greater particularity, the subject matter of the present invention and for clarifying certain antecedents used in the claim. For example, amended claim 15 recites that the isolation means ensures that operations performed by the input/output module and encryption module can be carried out in parallel in accordance with the teachings of the present invention. It will be noted that this language was both presented and considered previously in connection with earlier Office Actions. Applicants submit that the language is consistent with the teachings of the present invention. For example, in the illustrated embodiment of the present invention, the isolation means is described as being implemented by a dual port memory. Clearly, such a memory allows operations to be carried out in parallel as necessary such as when two devices access the memory at the same time. Accordingly, Applicants submit that the amendments made to claim 15 should not be deemed to raise new issues or necessitate a new search. If it is deemed desirable, Applicants are willing to amend the applicable portions of the specification to make this description clearer consistent with the translation of the priority document.

Also, Claim 29 was amended to clarify antecedents used in the claim and remove repetitive recitations included in the claim. Also, claims 18, 20 and 28 were amended to point out with greater particularity, the features of the CMOS memory. Other claims were amended for the purpose of providing proper antecedent basis for the elements recited therein. With these amendments, the claims should now be in proper form for allowance. For the reasons stated above, the amendments should not be deemed to raise new issues or necessitate a new search.

Applicants traverse the Examiner's rejection of claims 15-17 and 29-32 under 35 U.S.C. 103(a) as being unpatentable over US patent 4,604,683 to Russ et al in view of US

patent 6,021,201 to Bakhle et al. The Office Action states that Russ et al discloses an encryption circuit for simultaneously processing various encryption algorithms as set forth in claim 15. Applicants respectfully disagree for the following reasons.

Claim 15

According to the background of the invention section of the Russ et al patent, the invention is directed to an improved communications control unit useful for front end protocol processing of data communicated between a host processor and a communications network. Further, according to the Russ et al patent, it discloses architecture for avoiding microprocessor bus contention in favor of RAM contention for enhancing aggregate system performance. The Russ architecture is characterized by a central multiport random access memory (RAM) and microprocessor whose data transfer bus can be conceptually considered as segmented into multiple buses each connected to a different RAM port. Performance advantages in Russ are obtained in using multiple independent buses capable of performing operations concurrently and by shifting the traditional throughput limitations from microprocessor bus contention to RAM contention. According to Russ, RAM arbitration and RAM cycles are typically much faster than microprocessor bus arbitration and bus cycles.

The Russ et al patent further states that in accordance with an important aspect of the invention, the four bus segments can function independently of one another, thus allowing bus cycles on one bus to occur independently of cycles on any other bus. Additionally, Russ states that the RAM (i.e. memory array and related memory control logic) includes means for isolating the bus segments so that bus cycles occur independently of memory array cycles. That is, each bus segment can generate bus cycles and when these cycles do not require resources attached to other bus segments, the cycles can proceed independently of each other and also independently of the RAM. A further aspect of the Russ invention is that the RAM includes arbitration logic to establish priority between the bus segments competing for control of the RAM memory bus. Also, a stated significant feature of the Russ preferred embodiment is that microprocessor controlled bus interface circuits are provided to selectively connect or disconnect from one another, depending on the type of activity currently being executed.

From the above, it is seen that Russ teaches a front-end processor architecture for a host computer system. By contrast, claim 15 is directed to the architecture of an encryption circuit which can be used with a host computer system. The only connection to an interface other than that of the host processor is a serial link used for inputting basic keys through a secure path independent of the normal functional path (host computer bus) as defined in claims 30 and 31. Therefore, the elements 50, 51, 52, 54 and 56 cited in the Office Action which corresponds to a microprocessor and its resources connected to a CBus all form part of the front-end processor architecture and not an encryption circuit which is adapted to be coupled to a host computer system as recited in claim 15.

The control registers 56 of Russ cited as connecting the C Bus/microprocessor to the UNIBUS of the host computer via a dedicated bus are described as including a Unibus control and status register 204 and a Unibus vector register 206. These registers provide an interrupt capability that enables the host processor to interrupt the microprocessor via a multifunction peripheral (MFP) 54 for allowing the front-end processor to transfer a block of data from the Unibus memory to the multiport RAM. The actual data transfer requires the use of direct memory access controller (DMAC) 60 which is also required to be used for the transfer of data from the multiport RAM to the encryption unit located on the D Bus.

Thus, Applicants submit that Russ can not be said to provide an input/output module that couples to a host computer via a dedicated bus as defined in claim 15. By contrast, Russ discloses a microprocessor responsive to an interrupt caused by the host for enabling the front end processor (UPB) to transfer a block of data from the host UNIBUS memory to RAM via DMAC 60 and the DBUS port (see column 11, lines 32-54).

Furthermore, in distinguishing the description in Russ from the teachings of the present invention as defined in claim 15, the multiple bus arrangement and use of a single DMAC and a shared DBUS in Russ completely precludes any parallelism of the operations being performed by an input/output module (i.e. data exchanges between the module and the host computer system) and an encryption module (performing encryption and decryption operations) as defined in claim 15 because in Russ the same bus, the DBUS, is utilized for these two operations so they cannot proceed in parallel. Russ

illustrates this by the following examples of operations: The microprocessor unit connected to the CBUS can fetch an instruction from a read only memory also connected to the CBUS (operations confined to C Bus resources) while the DMA controller coupled to the DBUS is writing a word into a data encryption device also coupled to the DBUS. Concurrently, a second DMA controller coupled to the PBUS can write a word into the central RAM while a UNIBUS slave cycle takes place on the UBUS. Further, column 12, lines 62-65 state that in accordance with the preferred embodiment, only a single direct access controller is connected to each bus segment and thus, there is very little bus arbitration overhead or contention for the bus.

The Office Action cites the description discussed above in column 11, lines 37-62 relative to the data exchanges between the host (connected to the Unibus and U Bus) and encryption unit (D-Bus) as meeting the recitation in claim 15 of: the input/output module handles data exchanges between the host system and the encryption circuit. Applicants submit that this recitation is not met by the cited description for the following reasons. The cited description describes the host as initiating/causing a block transfer operation to take place by generating an interrupt and storing block transfer parameters in a set of software communications registers. It is only after the block has been transferred are there additional operations that may be performed which are application dependent. Such operations may involve processing by specific UPB peripheral components such as appending a checksum or encrypting the block of data is need are performed which are application dependent. These operations are performed by writing the block from RAM into either the checksum generator or the data encryption processor. Thus, in Russ, there are no data exchanges which generally occur between the microprocessor and the encryption processor. Russ shows a block transfer occurring between the host and RAM which is initiated by a host interrupt. Such transfer takes place under the control of DMAC 60 which then performs a read of the Unibus via the U bus and then a write to RAM via the D bus port.

As described in the cited material, if the block written to RAM needs to be encrypted, both the data encryption processor (DEP) 306 and the DMAC 60 will be initialized. The block will be read from memory in eight byte segments written into the DEP which will encrypt each segment and inform the DMAC when it is ready. Another

channel will then read the segment from the DEP and write it back to RAM. This operation will be repeated for each segment through the entire block. From this, it seems clear that the various data exchanges between the RAM and DEP are handled by the DMAC 60 and not the microprocessor as stated in the Office Action. Moreover, these exchanges in Russ are required to proceed serially through the RAM which allocates memory cycles on a priority basis. Applicants submit that this arrangement teaches away from the arrangement defined in claim 15 in which the encryption circuit of the present invention ensures that such operations can proceed in parallel.

The Office Action cites column 9, lines 25-60 as disclosing an encryption module which provides for the storage of all sensitive information of the encryption circuit. Applicants find the cited description to disclose a data encrypt and checksum processor 62 which is further described as including a data encrypt processor DEP 306 and a checksum generator 307. Appendix B lists an AmZ8068 Data Ciphering Processor described in the MOS Microprocessor and Peripherals Data Book Advanced Micro Devices. This is an integrated circuit chip that can be used to perform encryption or decryption. It is understood that to do both, two such chips would be required. The chip is used to provide a hardware implementation of the well-known DES algorithm. Since the cited circuit is a chip, there is no indication how such chips would be configured to carry out encryption and decryption operations and the management of sensitive data. Therefore, one would have to speculate what components are contained in the chip and how they would be configured to perform the operations specified in claim 15.

The Office Action cites column 2, lines 35-43 as disclosing a RAM configured for isolation means operatively connected between the input/output module and the encryption module, the isolation means configured to make sensitive information inaccessible to the host computer. In cited material contained in the summary of invention section of the Russ patent, the RAM is defined as including a memory array and control logic. Column 5, lines 43-59 of the Russ patent describe the arrangement of transceiver gates 80, 82, 84 and 86 for terminating each data bus segment and that the transceiver gates function to isolate the bus segments from the RAM array so that the bus cycle timing can be independent of the memory cycle timing of the RAM array.

By contrast and as discussed above, claim 15 defines isolation means connected between the input/output module and encryption module, the isolation means being configured to make the sensitive information stored in the encryption module inaccessible to the host computer system and ensures that the operations of the input/output module and encryption module can proceed in parallel. Clearly, this arrangement defined in claim 15 is not shown or suggested by the teachings of the Russ patent. As discussed above, the Russ patent teaches away from such parallelism. Also, as noted in the Office Action, as discussed herein, Russ does not disclose the storage of sensitive information, let alone making it inaccessible to a host system as defined in claim 15. Accordingly, in view of the above, Applicants submit that claim 15 as amended distinguishes patentably over the teachings of Russ.

As noted, the Office Action acknowledges that Russ is silent about sensitive information stored in the encryption module. As discussed above, since the chip provides a hardware implementation of the DES algorithm, there may be no need to incorporate sensitive information in such chip which is a consideration that involves management of sensitive information. Since Russ is primarily concerned with providing a front end processor, the handling of sensitive information relative to performing an encryption operation need not be addressed. In fact, it could be said that Russ teaches away from providing storage of sensitive information. As stated in the previously cited material in column 12 of the Russ, a block is encrypted only if it needs to be encrypted otherwise; the data encryption processor DEP 306 is not initialized. Thus, encryption is merely one of a number of options which further indicates that there is no need suggested to address the handling of sensitive information by the front end processor of Russ. Further, since the host system initiates a block transfer operation via an interrupt and supplies required parameters, it is logical to assume that the host would also supply encryption parameters for carrying out the encryption either prior to or when the block needs to be encrypted. By contrast, claim 15 is directed to an encryption circuit which is designed to carry out encryption operations for a host processor and not to a front end processor which may perform encryption. Further, there is suggestion that the host may provide the encryption parameters and therefore attempting to isolate its operation from the encryption processor

would be contrary to its teachings. This is an additional reason as to why claim 15 distinguishes patentably over the teachings of Russ.

The Office Action further cites the Bakhle patent as disclosing an input/output module, a dual port memory for performing parallel processing of different cryptographic operations and an encryption circuit which comprises a key storage unit for storing sensitive information as defined by Applicants claim 15. Applicants respectfully disagree. Applicants find Bakhle to disclose a cryptographic device 140 which includes a management processor (microprocessor) 142 responsible for providing data to device 140 via a system bus 145 using a direct memory access unit 144 to stream data into the device from a memory subsystem also connected to the system bus in common with processor and I/O subsystems. The device 140 contains a cipher unit 150 and hash unit 140 in addition to a security unit 250. The security unit 250 insures that the cipher unit 150 and the hash unit 154 operate on the same set of data (same data block) and that no new data is presented to the units until both units have completed the processing on the current block of data. The device 140 also includes a buffer unit 188 which includes a pair of buffers implemented with a triple ported register RAM capable of supporting two read ports and one write port.

As seen from the above, the parallelism provided in the Bakhle patent is relative to the processing of a single block wherein a cipher unit and a hash unit can operate on the same block for providing encryption and decryption services and for generating a hash value corresponding to the message. To do this, the cipher unit operates on a block of data having a first predetermined size and the hash unit operates on a data block having a second predetermined size. Thus, the operations while providing parallelism relative to processing a single block of data are unable to proceed independently of each other in that they are so limited by the security enhancement unit. In essence, the two units of Bakhle can be viewed as collectively performing a single encryption operation. As stated in the patent, the invention provides a single pass system (collective operations on each block of data at a time) in contrast to the prior art system of having a cipher unit process the message first and pass the message to a hash unit to perform the hash computation on the message. This differs from the teachings of the present invention relative to simultaneously processing various encryption algorithms as defined in claim

15. As an additional comment, one may view the hashing operation of Bakhle is not truly an encryption operation in that hashing is a transformation that takes an input and returns a fixed-size string which is called the hash value. It is normally a part of an encryption operation that authenticates a message or validates the encryption / decryption process, but is not in itself actually an encryption operation. Bakhle does not suggest any further parallelism of encryption processing.

Further, it will be noted that the operations of the cryptographic device require access to a stream of data from memory which is also illustrated in the system disclosed in Figure 7 of the patent. These different modes of operation and requirements, teach away from any attempt to modify or adapt the encryption circuit of Russ to provide storage in an encryption circuit as taught by Bakhle. That is, Bakhle contemplates the availability of a message source (a data stream) and therefore, for example, connects directly to the system bus in Figure 1 or directly to a source in Figure 7. By contrast, Russ provides for the connection of an encryption unit to memory via a low priority RAM port. Therefore, Applicants submit that to attempt to combine the teachings of the two patents as proposed in the Office Action could give rise to unpredictable results or lead to inoperability.

As concerns the storage of sensitive data, the RAM storage unit 164 of Bakhle is described as storing a plurality of keys with each key corresponding to a particular variation of the DES algorithm. The DES algorithm is a public algorithm that employs a single secret key for encryption and decryption and is a symmetric algorithm meaning that both the sender and receiver must know the secret key. The parties transmitting and receiving messages agree on the particular key to be used for communication. The present invention also provides support for encryption algorithms which are asymmetric and thus dependent on the secrecy of multiple private keys which can be stored for long periods within the isolated storage of the encryption unit. Keeping these keys secret from the host system provides a security and an operational advantage. Thus, Applicants submit that one could conclude that the storage provided in Bakhle does not contain the same sensitive information stored in the encryption module which is made inaccessible to the host computer system as specified in claim 15. It should be noted that it is the selection of the particular key to be used as agreed to by the parties that provides the

required security and that this key selection is made via a management processor issued command in Bakhle. It is also important to note that Bakhle does not discuss management of keys in terms of providing security or protection against access. But, rather Bakhle does discuss message authentication of messages using digital signatures. When security is discussed in Bakhle, it is relative to security unit 250 which increases the accuracy of the system by maintaining the atomicity of data blocks as discussed above by insuring that the cipher and hash units operate on the same set of data and that no new data is presented to such units until both have completed the processing on the current data block. Bakhle does not describe longer term storage of private keys or the loading of those keys from a source separated from the host system.

More importantly, it is seen that Bakhle does not provide for parallelism between the transfer of blocks of data and encryption operations for the reasons discussed above. Accordingly, for all of the above reasons, claim 15 should be deemed patentable over the proposed combination of the Russ and Bakhle patents. A notice to this effect is respectfully solicited.

Claim 16

Claim 16 distinguishes patentably over the combined references in providing isolation means which comprise a dual port memory. Figure 1 of the Russ patent cited in the Office Action discloses a multiport RAM which is shown in greater detail in Figure 2. As seen from Figure 2, the RAM 20 includes arbitration and control circuits 42 and a plurality of memory ports 22. The multiport RAM 20 is specifically designed to allocate memory access on a priority basis. According to the teachings of Russ, this is necessary for shifting the traditional throughput limited operations from microprocessor bus contention to RAM contention. Therefore, such an arrangement is unable to ensure the operations performed by the input/output module and encryption module can be carried out in parallel as defined in claim 15 upon which claim 16 depends. Also, the isolation in Russ is provided by a bus interface module 30 of Figure 2 which includes three tristate transceiver gates 140, 142, and 144 as stated in lines 10-15 of column 7. This module does not form part of multiport memory 20.

In view of the foregoing, Applicants submit that the combination of references cited in the Office Action does not show or suggest the arrangement defined by

dependent claim 16 directed to a dual port memory which operatively connects between the input/output module and the encryption module, is configured to make sensitive information stored in the encryption module inaccessible to the host computer system and ensures that the operations performed by the input/output module and encryption module can be carried out in parallel. Accordingly, claim 16 should be deemed patentable and a notice to this effect is respectfully solicited.

Claim 17

For the reasons given above relative to claim 16, claim 17 should also be deemed patentable over the proposed combination of references cited in the Office Action. Column 2, lines 35-43 of Russ cited in the Office Action discuss that the four bus segments can function independently of one another, thus allowing bus cycles on one bus to occur independently of cycles on any other bus. As stated in column 4 of Russ, when these buses do not require resources attached to other bus segments, the cycles can proceed independently. Therefore, when resources on the bus segments need to access the multiport memory 20 at the same time, there can not be independent bus cycles or cycles which are independent of the cycles of RAM 20 as taught by Russ (see column 4, lines 10-16). Further, as discussed above, the multiport RAM 20 arbitrates requests for memory cycles on a priority basis. Therefore, the multitport RAM 20 is unable to simultaneously handle exchanges of data, commands and status between the input/output and encryption modules as defined in claim 17.

The Office Action also cites column 9, lines 45-61 of Bakhle which describe the components of the security unit 250 as including an IN BUFFER which is a FIFO buffer implemented as a triple ported register RAM that supports two read ports and one write port. The security unit 250 controls buffer addressing which enables simultaneous addressing of odd and even banks of the IN BUFFER which can be read as a combination (64 bits) or individually (32 bits). This allows the cipher unit 150 to process 64 bits of data and the hash unit 154 to process 32 bits of data. As previously discussed, the security unit 250 ensures that the cipher unit 150 and hash unit 154 operate on the same set of data and that no new data is presented to both units until they both have completed processing on the current data block (see column 9, lines 14-19). Accordingly, it is seen that the security unit 250 is unable to provide simultaneous exchange of data, commands

and status between the input/output and encryption modules or isolation of these modules as defined in claim 17. Accordingly, for these reasons, claim 17 should be deemed patentable over the cited teachings of Bakhle.

Claim 29

This claim should be deemed patentable for the same reasons set forth relative to claim 15. Claim 29 defines that the input/output module comprises an input/output processor and PCI interface integrating DMA channels responsible for executing data transfers between the host computer system and the encryption circuit and that the input/output module memory comprises a flash memory containing the code of the input/output processor and a PCI interface integrating DMA channels and a static RAM that receives a copy of the contents of the flash memory upon startup of the input/output processor. This arrangement is not found in the portions of the Russ and Bakhle patents cited in Office Action.

More specifically, column 3, lines 59-65 of Russ describes the interface circuits 30, 32, and 34 of the front end processor which are used to establish connections between bus segments whenever the microprocessor 50 references a device not on the CBUS (see column 8, lines 11-14 and Figure 2). The cited lines 59-62 of column 4 describe the multifunction peripheral (MFP) device 54 as being used to generate timing signals and interrupts for devices without vector capability. Column 9, lines 1-7 describe the function of the system configuration register 200 as controlling the generation and detection of RAM parity, bus timeouts, and other status information. It describes LED/SW register 202 as a means of providing operator input/output, the UNIBUS control and status register UCSR 204 (a communications register) as controlling interaction with the UNIBUS principally DMA and interrupt capability (enables the UNIBUS acquisition logic 362) and the UVECT register 206 as containing a programmable UNIBUS interrupt vector applied to the UNIBUS when a grant is obtained by the UNIBUS acquisition logic 362.

Applicants submit that these citations neither show nor suggest an encryption circuit microcontroller that comprises an input/output processor and a PCI interface and a

flash memory, let alone integrating DMA channels responsible for executing data transfers between the host system and the encryption circuit.

The Office Action cites portions of the Bakhle patent as disclosing an encryption circuit in which a microprocessor comprises and input/output processor and a PCI interface and a flash memory, integrating DMA channels responsible for executing the data transfers between the host system and the circuit. By contrast, the cited material in column 4, lines 26-67 describes different subsystems and their components connected in common to a system bus 145 which also couples to a cryptographic device 140 which may alternatively couple to the systems I/O bus 158 or local bus within the host processor 111 of the system. The material describes the I/O subsystem of Figure 1 as including an I/O controller 131 acting as an interface between the I/O bus 158 and the system bus 145, providing a communication path for transferring information between devices coupled to different buses.

The material in column 5, lines 34-44 of Bakhle cited in the Office Action describes in greater detail, one of the components of the cryptographic device 140, namely the management processor (MP) 142 which connects to the system bus 146. According to the cited material, component MP142 shown in Figure 2 is responsible for providing data to an integrated hash and cipher unit referred to as a Bulk Cryptographic Cluster (BCC) 148 of device 140 which provides cryptographic services to MP142. As discussed in the cited material, software executing on the MP142 configures a direct memory access (DMA) 144 unit to stream data into the BCC 148 apparently from the memory subsystem.

From the above description, Applicants submit that the cited system does not disclose an encryption circuit which includes a microprocessor let alone a microprocessor which comprises an input/output processor and a PCI interface and a flash memory and DMA channels as defined in claim 29 in contrast to what is stated in the Office Action. Here, it is a management processor component of the cryptographic device 140 that streams data from memory and not a microprocessor component of an input/output module which is responsible for executing transfers between the host system and the encryption circuit as defined in claim 29. Accordingly, based on these differences, claim 29 should be deemed patentable over the cited portions of Bakhle.

The Office Action again cites column 4, lines 16-27 of Bakhle for disclosure of a flash memory containing the code of the input/output processor (i.e. lines 38-42) and an SRAM memory that receives a copy of the contents of the flash memory upon startup of the input/output processor (i.e. lines 26-67). The cited material describes that the memory subsystem 120 may include a memory controller 121 (which connects to the host system via the system bus) as controlling access to one or more devices 122 such as a DRAM, ROM, VRAM and the like. These memory devices store information for use by the host processor 121.

This arrangement of a computer system memory subsystem in Bakhle is completely different from that of an input/output module of an encryption circuit defined in claim 29. For example, there is no showing or suggestion of a flash memory storing code of the input/output processor let alone providing a copy of its contents to a static RAM upon startup of the input/output processor as defined in claim 29. In fact, Bakhle states to the contrary, the information contents of the memory devices are for use by the system **host processor**. Further, Applicants find no reference to instructions in the cited material as stated in the Office Action. Accordingly, for these additional reasons, claim 29 should be deemed patentable over the cited teachings of Bakhle. A notice to this effect is respectfully solicited.

Claims 30-31

The Office Action cites column 12, lines 48 through column 13, line 25 for disclosure of a card supporting the encryption circuit as defined in claims 30-31. It will be noted that in the illustrated embodiment of Applicants invention, the reference to card refers to the architecture of the encryption circuit embodied by a circuit supported by a PCI (Peripheral Component Interconnect) card. By contrast, the cited material in column 12 describes the operation of a data transaction system 330 of Figure 7 which is an entirely different embodiment from the system embodiment of Figure 1. As described in Bakhle, the data transaction system 330 has three components: data source 332, cipher and hash unit 148 and verification unit 336. As noted in the cited material, the data source 332 can be an ATM machine, a POS terminal or any other unit that takes data and forwards that data to verification unit 336. Further, the material states that the data source 332 provides plain text to the data transaction system 330 and is described as

including a keyboard, a magnetic reading device for reading a magnetic stripe on a card (e.g. ATM card or card) and a communication line (e.g. telephone line). Since any card reader that used as a data source 332 is required to provide plain text to the system 330, it should be clear that this path is not intended to be secure. Further, the example that the communication line being used is a telephone line provides additional evidence that such path is not secure as specified in claims 30-31.

Thus, Applicants find the cited material absent any disclosure of a dedicated PCI bus or a phone line for performing remote encryption operation and transmitting specific algorithm or a serial link that allows downloading of proprietary algorithms/keys into a first encryption submodule or that the serial link connected to input such keys is independent of the dedicated PCI bus as provided in claims 30-31. In fact, the cited material states that the data source provides plain text and such transmission would be controlled by the data source as is normally done in the described types of terminal transaction systems. This is in contrast to having such transmission being controlled by an encryption module as defined in claims 30-31. Also, since there is no dedicated bus used in the embodiment of Figure 7, there is no need to make the telephone communications path independent of a dedicated PCI bus as recited in claim 30. Accordingly, for the above stated reasons, claims 30-31 should be deemed patentable over the cited teachings of Bakhle.

Claim 32

For the reasons given above regarding claim 31, claim 32 should also be deemed patentable over the material cited in column 12, lines 47-65 of Bakhle discussed above. Applicants find no teaching in the cited material regarding including a card supporting an encryption circuit as defined in claim 32.

Claims 18 , 20-28 and 33-34

Applicants traverse the rejection of claims 18 and 20-28 and 33-34 under 35 USC 103(a) as being unpatentable over US patent 4,604,683 to Russ et al in view of US patent 6,021,201 to Bakhle et al as applied to claims 15-17 and further in view of IBM Technical Disclosure Bulletin, Cryptographic Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5. For the reasons given that claims 15-

17 distinguish patentably over the cited teachings of Russ and Bakhle, claims 18, 20-28 and 33-34 should also be deemed patentable.

Claims 18 and 20

Accordingly, for the reasons discussed above, Applicants disagree that as per claims 18 and 20 both cited references disclose the encryption circuit of claims 15-17 as stated in the Office Action. Relative to claims 18 and 20, the Office Action cites column 5, lines 14-67 and Figure 3 of Bakhle as disclosing an input/output module including a microcontroller and memory, a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms, and being coupled with a first bus of the dual-port memory; a second encryption sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled with the first bus of the dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory and including a separate internal second bus isolated from the first bus of the dual-port memory, performing parallel processing. Applicants find no such arrangement in Bahkle.

Also, Applicants disagree with the statements made in the Office Action that it would be obvious to modify the encryption circuit in Russ to provide first and second encryption modules for simultaneously performing various encryption algorithms as taught by Bakhle because one of ordinary skill in the art would be motivated to modify the encryption circuit of because of the suggestions in Bakhle of providing a cryptographic device capable of performing cryptographic operations in different formats while one type of operation is being performed another type can be performed concurrently or in parallel, for instance one cipher processor can operate on data having a first size whereas another processor can operate on a second block size. The Office Action cites column 5, lines 14-67, Figure 3 and column 1, lines 32-45 of Bakhle in support of these statements.

Column 5, lines 14-67 and Figure 3 have been discussed relative to the rejection of claim 15. It should be noted that lines 21-22 of column 5 state that the BCC 148 performs ciphering operations in parallel with hashing operations on a block of data. Bakhle also states that the ciphering and hashing operations occur concurrently or in parallel and are atomic (i.e. until both activities are complete, no reload of data is

permitted). From this, it is seen that Bakhle does not treat the operations being performed on a block of data as distinct independent different types of encryption operations. As stated in lines 44-49 of column 5, Bakhle describes the encryption software executing on the MP 142 as creating a digital signature using the hash value and appends it to the message. Also, lines 66-67 through column 6, line 3 describe the hash unit as including an input for receiving plain text and an output for providing a digital signature based on the plain text and that it does not operate on encrypted text. This description also treats the operations of the hash unit as being distinct from the encryption operations performed by the cipher unit.

Therefore in view of the above, Applicants submit that Bakhle does not teach an encryption module that comprises a first encryption sub-module, dedicated to the processing of symmetric encryption algorithms and a second encryption sub-module dedicated to the processing of asymmetric encryption algorithms as recited in claims 18 and 20. Also, Applicants find the cited material of Bakhle absent first and second encryption sub-modules being coupled to the first bus of the dual-port memory as defined in claims 18 and 20. Further, Applicants find the cited material of Bahkle absent a separate internal second bus isolated from the first bus of the dual-port memory as recited in the rejected claims. It should be noted that as defined by claims 18 and 20, the dual port memory is operatively connected between the input/output module and the encryption module. Therefore, the dual-port memory does not form part of the encryption module which would be the case in Bakhle if one were to equate the BCC input buffer components as including such elements. That is, as discussed in column 9 of Bakhle, the buffer unit included in the BCC 148 of Figure 3 cited in the Office Action, has an input buffer 190 and an output buffer 196, each of which is implemented by a tri-ported register RAM circuit. As seen from Figure 3, there is no first bus or internal second bus or connections to a dual port memory as specified in claims 18 and 20.

As to the motivation to combine the teachings of Bakhle and Russ as described in the Office Action, Applicants point out that Russ utilizes an encryption processor DEP 306 and a checksum generator 307 whose result is appended to a data block when needed. Thus, the checksum generator 307 can be likened to the hash unit whose result is appended to a message. As shown in Figure 6, both of the units 306 and 307 connect to

the DBUS which in turn connects both units to port 2 of the multiport RAM 20. As previously discussed, Russ teaches that when a checksum needs to be appended, a block from the RAM 20 will be written into the checksum generator 307. Also, when the block needs to be encrypted, the block will be read from RAM 20 in eight byte segments and written into FDEP 306 (see column 11, line 63 to column 12, line 11). Thus, Russ employs a mode of operation wherein either encryption processor DEP 306 or checksum generator 307 will receive blocks from port 2 of RAM 20. Since the same port is required to be used by both units, encryption and checksum generation can not be performed in parallel. This is apparently not necessary since these operations are only performed as needed. In view of the foregoing, even if one could modify Russ to incorporate the encryption and hash unit of Bakhle as proposed in the Office Action, there would be no advantages to do so in the system of Russ since such operations are performed only as needed and the cipher and hash units therefore must operate completely independently of each other. Further, the Bahkle cipher and hash units parallelism would not be possible since these units require simultaneous access to a block of data at a time while in the system of Russ, these units do not have parallel access to a block of data. Thus, unless there is a complete reconstruction and redesign of the Russ system, the Bakhle units could not be incorporated therein. Applicants submit that such obstacles to such reconstruction or redesign would dissuade a skilled artisan from being motivated to modify Russ in the manner proposed in the Office Action. Further, such reconstruction could only be accomplished by resorting to Applicants teachings which involves the hindsight reconstruction of the encryption circuit defined in claims 18 and 20.

It is noted that the material in lines 40-45 of column 1 cited in the Office Action pertains to ciphering algorithms and hash algorithms which characteristically operate on data having different block sizes. The Bakhle invention recognizes this fact and uses it to provide a storage unit having a size Q which is an integer multiple of M and N to accommodate the cipher unit which operates on a block of data having a first predetermined size M and the hash unit which operates on a data block having a second predetermined size N. Thus, Bakhle is seen not to teach providing a cryptographic device capable of performing cryptographic operations in different formats as stated in the

Office Action. In view of all of the foregoing, Applicants submit that claims 18 and 20 should be deemed patentable over the cited teaching and proposed combination of Russ and Bakhle.

The Office Action states that Russ does not explicitly disclose a CMOS memory which is coupled to the dual-port memory 4 via the first bus of the dual port memory, containing the encryption keys, for example, which is well known in the art. In support of this conclusion, the Office Action cites the invention disclosed in Dyke as implementing these elements in a security device. Applicants submit that the rejection of claims 18 and 20 in the Office Action is stated to be based on the teachings of three references: Russ, Bakhle and the cited IBM Disclosure Bulletin. To now cite the invention disclosed in another reference, Dyke, is inconsistent with the present stated rejection. Moreover, Applicants submit that the inclusion of Dyke makes the rejection improper. A further problem is that an earlier rejection dated August 2, 2007 states relative to the rejection of claims 18-20 that Dyke does not explicitly disclose a CMOS memory which is coupled with the dual port memory containing the encryption keys. Lastly, in regard to this rejection is that the Office Action states that it would have been obvious to one of ordinary skill in the art of computer security to modify the **circuit of** as combined above to provide a CMOS memory coupled with the dual port memory via the first bus of the dual port memory containing the encryption keys as taught in the IBM Technical Disclosure Bulletin. Obviously, some words have been omitted from the rejection rendering the rejection incomplete. That is, it is not known what circuit is being cited and what elements are being combined to render claims 18 and 20 obvious. Accordingly, Applicants request clarification of the grounds for the present rejection of claims 18 and 20. This same request also applies to claim 28 since the Office Action also cites the Dyke patent in the rejection of this claim.

Before discussing the cited material to the extent that the rejection is understood, Applicants point out that claims 18 and 20 have been amended to point out with greater particularity the aspects of the present invention related to the use of a CMOS memory. As amended, claims 18 and 20 now define that the CMOS memory is accessible during execution of encryption algorithms by the first and second encryption sub-modules and that the CMOS memory is connected to be reset upon detection of an alarm condition for

protecting the encryption keys from unauthorized access and use consistent with the teachings contained in Applicants specification. Also, the claims have been amended to even better clarify that the CMOS memory contains the encryption keys in view of the Office Action reference in the rejection that the dual-port memory containing the encryption keys.

The Office Action references the IBM Disclosure Bulletin as supporting well known art by disclosing a single chip microcontroller comprising a flash memory, a data RAM memory and a CMOS memory. Applicants find the IBM Disclosure Bulletin to disclose a solution for protecting the loadable microcode of a microcontroller which involves the encrypting the microcode for transportation and storage and decrypting the microcode only within the confines of the microcontroller itself. The solution is implemented in Figure 1 wherein the microcode ROM is split into two segments (both ROM and RAM or EEPROM) and a new storage element (key storage) is defined. The smaller ROM which is common to all devices, would have bootstrap and decryption microcode and be used for initializing and "IPLing" (Initial Program Loading which is the process of copying an operating system into memory when a system is booted) the microcontroller. This would load the encrypted microcode into a microcode RAM or EEPROM, decrypt it and begin execution. To allow the decryption of the microcode by the microcontroller, the decryption key would be kept in the key storage element. The cited Disclosure Bulletin suggests additional security measures for protection of the microcode and key storage after having been loaded. Such measures relate to the type of chip fabrication/coating methods and the use of a CMOS RAM with battery backup. However, it should be noted that the IBM Disclosure Bulletin specifically states that the subject of key distribution and management is quite complicated and has not been dealt with by the disclosure.

In view of the above, Applicants find the IBM Disclosure Bulletin to be directed to the protection of encrypted microcode and not to encryption of data as defined in claims 18 and 20. Further, there is only a disclosure of a microcontroller that performs decryption of encrypted microcode and of security measures which involves the use of CMOS memory for storing a decryption key. By contrast, claims 18 and 20 provide a CMOS memory which is accessible during execution of encryption algorithms by the

first and second encryption sub-modules and that the CMOS memory is connected to be reset upon detection of an alarm condition for protecting the encryption keys from unauthorized access and use. Clearly, this arrangement is neither shown nor suggested by the IBM Disclosure Bulletin. The requirement for battery backup would not be relevant in the case of the present invention which provides a different approach. In view of the foregoing, Applicants submit that claims 18 and 20 should be deemed patentable over the cited references. A notice to this effect is respectfully solicited.

Claim 21

Before discussing the rejection of claim 21, it will be noted that claim 21 has been amended to clarify that the two encryption processors couple to the first bus of the of the dual-port memory so as to be consistent with the remainder of the claim. Relative to the rejection, Applicants submit that claim 21 should be deemed patentable for the same reasons as set forth for claim 18. The Office Action in support of such rejection cites the same material in column 5, lines 14-67 as cited in the rejection of claim 18. Additionally, the Office Action cites Figures 3-6 with description and table 2, column 8, column 13, lines 10 et seq. relative to the disclosure of a control unit that comprises a security unit that controls input and output and uses buses separate from the dual port bus and meets the recitation of and a bus isolator for isolating the second bus from the first bus of the dual port memory. Applicants find the cited material to describe the BCC 148, its security unit 250 shown in Figure 6, an encryption mode operation depicted in Figure 4 and a decryption mode of operation depicted in Figure 5. As to the Office Action statement phrase "meets the recitation of and a bus isolator", Applicants find such phrase incomplete in that it does not identify completely the recitation in claim 21 that is met. It is possible that the"and" is intended to be omitted from the phrase. Accordingly, based on this interpretation of the rejection, Applicants find cited table 2 to provide the definition of signals internal to the cryptographic device 140 of Figure 2, the cited column 8 to describe the processing steps of the flow chart of Figure 5 in carrying out a decryption operation and column 13, lines et seq. to describe the flow chart of Figure 8 illustrating the operations of how a control device accesses the BCC 148 of device 140.

Applicants find the cited descriptions absent a disclosure of a bus isolator which operates as defined in claim 21. The security unit 250 is described in Bakhle as

controlling the sequencing of the hash and cipher data paths through the proper datasets as well as generating a DONE signal to indicate to the DMA that BCC 148 is finished with the current data block and is ready to accept the next data block as described in column 6. The interface signals employed by the control device (e.g. MP 142) to interface with the BCC 148 are shown in Table 1. As seen from the table, the interface signals include a bidirectional data bus (external bus) which is used to provide the data signals ID(33) via the control unit 160 to the IN BUFFER 190 and receive the data signals OD(32) from the OUT BUFFER 196 via control unit 160. From this, it seen from the cited descriptions that they disclose a single external bus associated with the control unit 160 and an absence of isolation circuits since BCC 148 includes separate in and out buffer circuits 190 and 196 which make isolation unnecessary. Also, Applicants find the cited descriptions absent and encryption component and at least two encryption processors, the encryption component coupled to the first bus of a dual port memory and the two encryption processors being coupled to the first bus via the second internal bus of the second sub-module wherein a bus isolator isolates the second bus from the first bus of the dual port memory as defined in amended claim 21.

Further, Applicants find the cited descriptions absent of any disclosure of an encryption component dedicated to the processing of symmetric encryption algorithms and at least two encryption processors dedicated to the processing of asymmetric encryption algorithms. As discussed above, Bakhle teaches use of a single encryption (cipher) processor and a hash unit which performs a distinctly different type of operation. Applicants find no suggestion in the cited end of column 5 that the encryption processor and hash unit can be implemented with specific dedicated hardware components known in the art for the processing of asymmetric and symmetric algorithms as stated in the Office Action. In fact, the description at the end of column 5 states that reference may be made to a 1996 publication for disclosure of the specific algorithms used to determine the functionality of both the cipher unit and the hash unit. Such description can not be properly interpreted to mean that the functions of such units are to be changed as stated in the Office Action.

The cited description also states relative to the use of specific dedicated hardware components for encryption and decryption that one skilled in the art knows that the cipher

unit 150 can be implemented using such components or as a software routine. As to the hash unit 154, the cited description states that the hash unit 154 can implemented with dedicated hardware components or as a software routine. In other words, the cited material simply states that these units in Bakhle can be implemented in hardware or in software as will be understood by one skilled in the art. The cited description goes on to note that the hash unit includes an input for receiving plain text and an output for providing a generated digital signature in addition to not operating on ciphertext (encrypted text). This description further evidences intent not to change the functionality of such units. In view of all of the foregoing, Applicants submit that claim 21 should be deemed patentable over the cited descriptions of Bakhle. A notice to this effect is respectfully solicited.

Claims 22-23 and 25

Relative to the rejection of claims 22-23 and 25, Applicants submit that such claims should be deemed patentable for the same reasons as set forth for claim 18. The Office Action in support of such rejection cites the same material in column 5, lines 14-67 as cited in the rejection of claim 18. Applicants submit for the reasons given above relative to claim 21, the cited description in column 5, lines 50-67 does not show or suggest the use of different algorithms let alone the CIP and ACE configurations for encryption processors and the SCE configuration for the encryption component as defined in claims 22-23 and 25. As to having both processors CIP configured being a matter of design choice, the cited description of Bakhle in column 5 suggest the contrary. It indicates the selection of the DES encryption algorithm and MDS/SHA hashing algorithms. Clearly, this provides further evidence as to the choice of algorithms by Bakhle which is in contrast to the configuration algorithms defined in claims 22-23 and 25. In view of the foregoing, Applicants submit that claims 22-23 and 25 should be deemed patentable over the cited descriptions in Bakhle. A notice to this effect is respectfully solicited.

Claims 24 and 26

Relative to the rejection of claims 24 and 26, Applicants submit that such claims should be deemed patentable for the same reasons as set forth for claim 18. The Office Action acknowledges that Bakhle does not explicitly disclose that one of the processors

and the encryption component comprises a FPGA. The Office Action cites column 9, lines 55 et seq. relative to the disclosure of input output buffer arrays and cites the end of column 5 discussed above for disclosure that the cipher and hash units can be implemented with specific dedicated hardware components known in the art for processing of asymmetric and symmetric algorithms. For the reasons given with respect to claims 21, 22-23 and 25, claims 24 and 26 should be deemed patentable over the cited Bakhle. It should be noted that relative to the input and output buffers, Bakhle in columns 9 and 11 that the input buffer 190 is a FIFO buffer implemented as a triple ported register RAM that is capable of supporting two read ports and one write port and that the output buffer 196 is a triple ported register RAM capable of supporting two read ports and one write port. Clearly, this description shows that Bakhle teaches the use of different hardware components in contrast to those defined in claims 24 and 26. Further, it should be noted that the storage function provided by the input and output buffers of Bakhle are in contrast to the encryption functions provided by a field programmable gate array defined in claims 24 and 26. These differences in construction and in function would dissuade one skilled in the art from attempting to implement such encryption functions with the cited components of Bakhle. In view of the foregoing, Applicants submit that claims 24 and 26 should be deemed patentable. A notice to this effect is solicited.

Claim 27

This claim defines the second sub-module as comprising a flash memory PROM and an SRAM memory coupled to the second internal bus of the sub-module. Applicants find this arrangement absent from the description contained in page 2 and Figure 1 of the IBM Disclosure Bulletin cited in the Office Action. As discussed relative to claims 18 and 20, the Bulletin discloses a solution for protecting the loadable microcode of a microcontroller which involves the encrypting the microcode for transportation and storage and decrypting the microcode only within the confines of the microcontroller itself.

As discussed above, the solution is implemented in Figure 1 of the Bulletin wherein the microcode ROM is split into two segments (both ROM and RAM or EEPROM) and a new storage element (key storage) is defined. The smaller ROM which

is common to all devices, would have bootstrap and decryption microcode and be used for initializing and "IPLing" (Initial Program Loading which is the process of copying an operating system into memory when a system is booted) the microcontroller. This would load the encrypted microcode into a microcode RAM or EEPROM, decrypt it and begin execution. To allow the decryption of the microcode by the microcontroller, the decryption key would be kept in the key storage element. From the foregoing, it is seen that cited memory components are not used to perform encryption, let alone encryption involving data exchanges as defined in claim 27 and the claims from which claim 27 depends (i.e. claim 15). As to the selection of components being a matter of design choice, Applicants point out that the cited Bulletin suggests the contrary by making a choice of using ROM and RAM which could be CMOS RAM or EEPROM rather than the flash memory PROM and an SRAM memory for the second encryption sub-module coupled to the second internal bus of the sub-module as specified in claim 27. In view of the foregoing, Applicants submit that claim 27 should be deemed patentable. A notice to this effect is respectfully, solicited.

Claim 28

Before discussing the rejection, Applicants point out that claim 28 has been amended to more particularly define the aspects of the claimed invention. Relative to the rejection of claim 18, Applicants submit that claim 28 should be deemed patentable for the same reasons as set forth for claim 18. Also, for the reasons given regarding the rejection of claims 18 and 20 relative to the citation of Dyke, Applicants find the basis of the rejection of claim 28 improper and request clarification. Applicants find the cited material absent a disclosure of an encryption circuit comprising a CMOS memory containing security keys and security mechanisms that trigger a reset mechanism of the CMOS memory in case of an alarm as defined in claim 28. As to the cited IBM Disclosure Bulletin, as discussed above, the CMOS memory is suggested for use implementing the key store and the microcode store because of its sensitivity to light and static charge which would make probing or examination difficult. Further, the cited Bulletin suggests that such RAMs could be backed up with a battery when the system was unpowered. Thus, the Bulletin contemplates that these RAMs maintain their contents intact and not be resettable as set forth in claim 28.

As concerns the citation of the Dyke patent, notwithstanding a request for further clarification as to the grounds of rejection, Applicants have reviewed the cited material in column 8, lines 25-32 and 63-67. The descriptions in lines 25-32 and 63-67 pertain to operations that occur in response to instructions issued by a ROM initialization routine which provide a software reset command to the DES chip, to clear different flags and thereafter when the host processor has information to be encrypted or decrypted, the encryption mode or decryption mode is selected for the DES chip followed by the issuance of a load DES master key command for loading the DES master key register with data from the dual port RAM (DPR). From this, it is seen that Dyke provides the capability of issuing a software reset of the DES chip in contrast to resetting a CMOS memory containing security keys and security mechanisms that trigger a reset mechanism of the CMOS memory in the case of an alarm as recited in claim 28. Further, in Dyke, the cited DES reset operation occurs following the start of the operation of the encryption board in response to a ROM initialization routine which can be likened to a power on or startup sequence. By contrast, the reset mechanism of claim 28 is not triggered during normal operation but rather in the case of an alarm causing the contents of the CMOS memory to be destroyed thereby protecting its contents from use or access. This clearly is opposite to the cited teachings of the Dyke patent.

In view of the foregoing, Applicants submit that claim 28 should be deemed patentable. A notice to this effect is respectfully solicited.

Claims 33-34

Applicants submit that claims 33-34 directed to the encryption circuit further including a supporting card, should be deemed patentable for the reasons set forth relative to the rejection of claims 30-32. As previously stated, Applicants find the description contained in column 12, lines 47-65 absent any disclosure of a card supporting the encryption circuit. Applicants submit that the fact that the data transaction system of Figure 7 may use a magnetic reading device for reading a magnetic stripe on a card does not suggest that such card supports an encryption circuit. In fact, if one could broadly interpret such language to suggest support, it would be that the card would be viewed as providing support to the magnetic reading device. For these reasons, Applicants submit

that claims 33-34 should be deemed patentable. A notice to this effect is respectfully solicited.

In view of the above arguments and clarifying amendments, Applicants submit that claims 15-18 and 20- 34 should be deemed patentable over the cited prior art. A notice to this effect is respectfully solicited. Applicants ask the Examiner to contact Applicants attorney to discuss the grounds for rejecting Applicants claims before acting on this amendment. Also, if any questions or issues should arise with respect to this amendment or the allowability of this application, the Examiner is urged to call Applicants' representative at the number indicated herein. Further, if the Examiner feels that a discussion will further advance the prosecution of this application, the Examiner is also urged to call as suggested herein.

Respectfully submitted,

Russell W. Guenthner

Russell W. Guenthner, Ph.D.
Reg. # 54,140